Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method of processing out-of-order message[[s]] packets, comprising:

obtaining ~~determining, with a secure communication module of a receiving client device,~~ a maximum largest nonce value ~~yet seen from a plurality of nonce values of out-of-order messages~~;

comparing, with said secure communication module of said receiving client device, a nonce value of a received out-of-order message packet with ~~said~~ a largest nonce value yet seen;

comparing, with said secure communication module of said receiving client device, ~~said nonce value to nonce values within a single replay attack acceptance window in response to said nonce value not exceeding~~ said largest nonce value yet seen with said maximum largest nonce value; ~~adjusting, with said secure communication module of said receiving client device, a size of a range of acceptable nonce values within said single replay attack acceptance window, where said size of said range is based on said determined largest nonce value yet seen;~~ and

resetting said largest nonce value yet seen and generating a new cryptographic key when said largest nonce value yet seen exceeds said maximum largest nonce value ~~rejecting, with said secure communication module of said receiving client device, said received out-of-order message if said nonce value falls outside said single replay attack acceptance window~~.

2. (previously presented) The method according to claim 1, further comprising:

designating, with said secure communication module of said receiving client device, said nonce value as said largest nonce value yet seen if said nonce value exceeds said largest nonce value yet seen.

3. (previously presented) The method according to claim 1, further comprising:

replacing, with said secure communication module of said receiving client device, said largest nonce value yet seen with said nonce value if said nonce value exceeds said largest nonce value yet seen.

4. (previously presented) The method according to claim 1, further comprising:

adjusting, with said secure communication module of said receiving client device, ~~said~~ a single replay attack acceptance window if said nonce value exceeds said largest nonce value yet seen.

5. (currently amended) The method according to claim 1, further comprising:

designating, with said secure communication module of said receiving client device, said received out-of-order message packet as a replay attack.

6. (currently amended) The method according to claim 1, further comprising:

comparing, with said secure communication module of said receiving client device, said nonce value to a window mask value if said nonce value falls within said single replay attack acceptance window; and

rejecting, with said secure communication module of said receiving client device, said received out-of-order message packet if said nonce value is within said window mask value.

7. (currently amended) The method according to claim 6, further comprising:

designating, with said secure communication module of said receiving client device, said received out-of-order message packet as part of a replay attack.

8. (currently amended) The method according to claim 1, further comprising:

comparing, with said secure communication module of said receiving client device, said nonce value to a window mask value if said nonce value falls within said single replay attack acceptance window; and

accepting, with said secure communication module of said receiving client device, said received out-of-order message packet if said nonce value is outside said single replay attach acceptance window.

9. (previously presented) The method according to claim 8, further comprising:

designating, with said secure communication module of said receiving client device, said nonce value as a largest nonce value yet seen.

10. (currently amended) An apparatus for processing out-of-order message[[s]] packets, said apparatus comprising:

a receiving communication interface configured to transmit and receive a plurality of packets; and

a receiving controller, wherein said receiving controller is configured to:

obtain ~~determine~~ a maximum largest nonce value ~~yet seen from a plurality of nonce values of out-of-order messages~~;

compare a nonce value of a received out-of-order message packet and ~~said~~ a largest nonce value yet seen;

compare said largest nonce value yet seen ~~to nonce values within a single replay attack acceptance window in response to said nonce value not exceeding~~ with said maximum largest nonce value ~~yet seen~~; ~~adjust a size of a range of acceptable nonce values within said single replay attack acceptance window, where said size of said range is based on said determined largest nonce value yet seen;~~ and

resetting said largest ~~reject said received out-of-order message if said~~ nonce value ~~falls outside said single replay attack acceptance window~~ yet seen and generating a new cryptographic key when said largest nonce value yet seen exceeds said maximum largest nonce value.

11. (previously presented) The apparatus according to claim 10, wherein:

said receiving controller is further configured to designate said nonce value as said largest nonce value yet seen if said nonce value exceeds said largest nonce value yet seen.

12. (currently amended) The apparatus according to claim 10, wherein:

said receiving controller is further configured to adjust ~~said~~ a single replay attack acceptance window if said largest nonce value yet seen exceeds said largest nonce value yet seen.

13. (previously presented) The apparatus according to claim 10, wherein:

said receiving controller is further configured to replace said largest nonce value yet seen with said nonce value if said nonce value exceeds said largest nonce value yet seen.

14. (currently amended) The apparatus according to claim 10, wherein:

said receiving controller is further configured to designate said received out-of-order message packet as part of a replay attack.

15. (currently amended) The apparatus according to claim 10, wherein said controller is further configured to:

compare said nonce value to a window mask value if said nonce value falls within ~~said~~ a single replay attack acceptance window; and

reject said received out-of-order message packet if said nonce value falls outside said single replay attack acceptance window.

16. (currently amended) The apparatus according to claim 15, wherein:

said receiving controller is further configured to designate said received out-of-order message packet as part of a replay attack.

17. (currently amended) The apparatus according to claim 10, wherein said controller is configured to:

compare said nonce value to a replay attack acceptance window value if said nonce value falls within said single replay attack acceptance window; and

accept said received out-of-order message packet if said nonce value falls within said single replay attack acceptance window.

18. (previously presented) The apparatus according to claim 17, wherein:

said receiving controller is further configured to mark said nonce value as said largest nonce value yet seen.

19. (currently amended) A non-transitory computer readable storage medium on which is embedded one or more computer programs, said one or more computer programs implementing a method of processing out-of-order message[[s]] packets, said one or more computer programs comprising a set of instructions for:

obtaining ~~determining, with a secure communication module of a receiving client device~~, a maximum largest nonce value ~~yet seen from a plurality of nonce values of out-of-order messages~~;

comparing, with said secure communication module of said receiving client device, a nonce value of a received out-of-order message packet and ~~said~~ a largest nonce value yet seen;

comparing, with said secure communication module of said receiving client device, ~~said nonce value to nonce values within a single replay attack acceptance window in response to said nonce value not exceeding~~ said largest nonce value yet seen with said maximum largest nonce value; ~~adjusting, with said secure communication module of said receiving client device, a size of a range of acceptable nonce values within said single replay attack acceptance window, where said size of said range is based on said determined largest nonce value yet seen;~~ and

resetting said largest nonce value yet seen and generating a new cryptographic key when said largest nonce value yet seen exceeds said maximum largest nonce value ~~rejecting, with said secure communication module of said receiving client device, said received out-of-order message if said nonce value not falls within said single replay attack acceptance window~~.

20. (previously presented) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

designating, with said secure communication module of said receiving client device, said nonce value as said largest nonce value yet seen if said nonce value exceeds said largest nonce value yet seen.

21. (previously presented) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

replacing, with said secure communication module of said receiving client device, said largest nonce value yet seen with said nonce value if said nonce value exceeds said largest nonce value yet seen.

22. (currently amended) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

adjusting, with said secure communication module of said receiving client device, ~~said~~ a single replay attack acceptance window based on said nonce value if said nonce value exceeds said largest nonce value yet seen.

23. (currently amended) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

designating, with said secure communication module of said receiving client device, said received out-of-order message packet as a replay attack.

24. (currently amended) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

comparing, with said secure communication module of said receiving client device, said nonce value to a window mask value if said nonce value falls within ~~said~~ a single replay attack acceptance window; and

rejecting, with said secure communication module of said receiving client device, said received out-of-order message packet if said nonce value falls outside said single replay attack acceptance window.

25. (currently amended) The computer readable storage medium in according to claim 24, said one or more computer programs further comprising a set of instructions for:

designating, with said secure communication module of said receiving client device, said received out-of-order message packet as part of a replay attack.

26. (currently amended) The computer readable storage medium in according to claim 19, said one or more computer programs further comprising a set of instructions for:

comparing, with said secure communication module of said receiving client device, said nonce value to a window mask value if said nonce value falls within ~~said~~ a single replay attack acceptance window; and

accepting, with said secure communication module of said receiving client device, said received out-of-order message packet if said nonce value falls within said single replay attack acceptance window.

27. (previously presented) The computer readable storage medium in according to claim 26, said one or more computer programs further comprising a set of instructions for:

designating, with said secure communication module of said receiving client device, said nonce value as said largest nonce value yet seen.

28. (currently amended) A system for processing out-of-order message[[s]] packets in a peer-to-peer configuration, comprising:

a first peer configured to provide secure communication;

a second peer configured to provide said secure communication; and

a receiving secure communication module configured to be executed by said first peer and second peer, wherein said receiving secure communication module is configured to:

obtain ~~determine~~ a maximum largest nonce value ~~yet seen from a plurality of nonce values of a out-of-order messages~~;

compare a nonce value ~~to a filter in response to said nonce value~~ of a received out-of-order packet ~~not exceeding said~~ a largest nonce value yet seen;

compare said largest nonce value yet seen with said largest nonce value ~~to nonce values within a single replay attack mask~~; ~~adjust a size of a range of acceptable nonce values within said single replay attack mask, where said size of said range is based on said determined largest nonce value yet seen;~~ and

reset said largest nonce value yet seen and generate a new cryptographic key when said largest nonce value yet seen exceeds said maximum largest nonce value ~~accept said received out-of-order packet if said nonce value falls within said single replay attack mask~~.

29. (previously presented) The system according to claim 28, wherein:

said receiving secure communication module is further configured to designate said nonce value as said largest nonce value yet seen if said nonce value exceeds said largest nonce value yet seen.

30. (currently amended) The system according to claim 28, wherein:

said receiving secure communication module is further configured to adjust ~~said~~ a single replay attack mask based on said largest nonce value yet seen if said nonce value exceeds said largest nonce value yet seen.

31. (currently amended) The system according to claim 28, wherein:

said receiving secure communication module is further configured to reject said received out-of-order packet if said nonce value falls outside ~~said~~ a single replay attack mask.

32. (previously presented) The system according to claim 31, wherein:

said receiving secure communication module is further configured to designate said received out-of-order packet as part of a replay attack.

33. (currently amended) The system according to claim 32, wherein:

said receiving secure communication module is further configured to reject said received out-of-order packet if said nonce value falls outside ~~said~~ a single replay attack mask.

34. (previously presented) The system according to claim 33, wherein:

said receiving secure communication module is further configured to designate said received out-of-order packet as part of a replay attack.

35. (currently amended) The system according to claim 28, wherein:

said receiving secure communication module is further configured to reject said received out-of-order packet if said nonce value falls outside ~~said~~ a single replay attack mask; and

said receiving secure communication module is further configured to designate said received out-of-order packet as part of a replay attack.

36. (currently amended) A receiving interceptor device for processing out-of-order message[[s]] packets, said receiving interceptor device comprising:

a network interface;

an expected sequence register configured to enumerate an expected sequence number of a message packet received out-of-order from a second network device; ~~a memory configured to store a single replay attack mask;~~ and

a receiving controller, wherein said receiving controller is configured to:

obtain ~~determine~~ a maximum largest nonce value ~~yet seen from a plurality of nonce values of out-of-order messages~~;

compare a nonce value ~~to a filter in response to a sequence number~~ of a received out-of-order message packet with a ~~via said network interface does not exceed said~~ largest nonce value yet seen ~~retrieved from said expected sequence register~~;

compare said largest nonce value yet seen with said maximum largest nonce value ~~sequence number to said single replay attack mask retrieved from said memory; adjust a size of a range of acceptable nonce values within said single replay attack mask, where said size of said range is based on said determined largest nonce value yet seen~~; and

reset said largest nonce value yet seen and generate a new cryptographic key when said largest nonce value yet seen exceeds said maximum largest nonce value ~~accept said received out-of-order packet if said sequence number falls within said single replay attack mask~~.

37. (previously presented) The receiving interceptor device according to claim 36, wherein:

said controller is further configured to designate said sequence number as said largest nonce value yet seen if said sequence number exceeds said largest sequence number yet seen.

38. (previously presented) The receiving interceptor device according to claim 36, wherein:

said controller is further configured to adjust said single replay attack mask based on said largest nonce value yet seen if said sequence number exceeds said largest nonce value yet seen.

39. (currently amended) The receiving interceptor device according to claim 36, wherein:

said controller is further configured to reject said received out-of-order packet if said sequence number falls outside ~~said~~ a single replay attack mask.

40. (previously presented) The receiving interceptor device according to claim 36, wherein:

said controller is further configured to designate said received out-of-order packet as part of a replay attack.

41. (currently amended) The receiving interceptor device according to claim 36, wherein:

said controller is further configured to reject said received out-of-order packet if said sequence number falls outside ~~said~~ a single replay attack mask.

42. (previously presented) The receiving interceptor device according to claim 41, wherein:

said controller is further configured to designate said received out-of-order packet as part of a replay attack.

43. (currently amended) The receiving interceptor device according to claim 36, wherein:

said controller is further configured to reject said received out-of-order packet if said sequence number falls outside ~~said~~ a single replay attack mask; and

said controller is further configured to designate said received out-of-order packet as part of a replay attack.